

### **REMARKS**

These remarks are directed to the office action mailed August 1, 2008, setting a three month shortened statutory period for response set to expire on November 1, 2008. The office action issued by the Examiner and the citations referred to in the office action have been carefully considered.

Prompt reconsideration is requested in view of the above claim amendments and the following remarks. As indicated, amendments introduce no new matter. Claims 1-2, 4-6, and 8-12 are currently pending.

### **Drawings**

Figure 1 has been amended to include reference to the machine readable zone, labeled "MRZ". Support for this amendment is found on page 7, line 5 of Applicant's specification. No new matter has been added.

### **Claim Rejections under 35 USC § 103**

Claims 1-2, 5-12, and 15-19 have been rejected under 35 USC §103(a) as being unpatentable over Burger (U.S. Patent 6,219,439) in view of Trench (U.S. Patent Publication No. 2005/0154877 A1) and in further view of Chen et al. (U.S. Patent 5,694,471).

Applicant respectfully submits that the Examiner may not have fully understood Applicant's verification system and process. The system and process comprises of four main steps in verifying and authenticating a document and the document holder.

#### **1. Authentication of the chip in the document.**

The chip contains private keys, a biocertificate, and data with a predetermined relationship to the holder details. The processing unit (CPU) transmits a random challenge code to the chip, which is then digitally signed by the chip using a

private key and sent back to the CPU. The CPU authenticates the chip by comparing the digitally signed challenge code with a certificate from the issuing authority.

2. Authentication of the biocertificate.

The biocertificate contains biometric data of the holder. Similar to the authentication process for the chip, a digitally signed biocertificate using a private key is sent to the CPU. The CPU authenticates the biocertificate by comparing the digitally signed biocertificate with a certificate from the issuing authority.

3. Authentication of the holder.

Biometric features of the holder are scanned. The CPU authenticates the holder by comparing the scanned biometric features with the digitally signed biocertificate, which contains the biometric data on the holder.

4. Authentication of the holder details.

The data with a predetermined relationship to the holder details were generated by a one-way function. The CPU authenticates the holder details by comparing the data with the holder details. The purpose of having the holder details separate from the biocertificate is so that the biometric data of the holder would not be directly linked to the holder details.

The Examiner cites 3 references: Burger, Trench, and Chen. Burger deals with Step 3. Authentication of the holder. Trench deals with Step 1. Authentication of the chip. The Examiner states in the office action that “they do not teach verifying the authenticity of the data itself...” (page 7, second paragraph), namely, Burger and Trench teach nothing regarding steps 2 and 4.

Chen teaches a complex card authentication process that is neither similar to Step 2 nor Step 4. As described in column 9, line 50 to column 10, line 11 of Chen:

“...the first step in the card authentication process (step 200) is for the card holder or user to insert the card into the processing terminal, whereupon the terminal retrieves the record from the card, using pointers if necessary, based on the issuer ID number stored on the card and associated with the relevant record (step 210).

The transaction processing terminal then decrypts the record's digital signature (step 220) using the public key Kpu stored in the record to obtain the composite result  $(D.sub.Kpu [DS]=D.sub.Kpu [E.sub.Kpr (CR)]=CR$ , where D represents the deciphering operation and E represents the encryption operation described above which was performed during card initialization). The composite result is then XORed with the card's unique serial number to obtain a recovered checksum (step 230), and another checksum is computed directly from the information record by running the issuer ID and public key through a one-way hashing function, just as was done to create the original checksum which, assuming that the digital signature is secure, will be the same as the recovered checksum (step 240). The resulting checksums are then compared (steps 250 and 260) and if either the digital signature or the information record was altered, the results will not match and the card is rejected (step 270) or confiscated. If the checksums match, the card record is authenticated.”

As described in Chen, a card record is authenticated by comparing a recovered checksum to another checksum. The recovered checksum is generated by a complex process of first decrypting a digital signature with a public key and then XOR with the card's serial number. The other checksum is generated by hashing an issuer ID with a public key. Applicant's step 2 and 4 do not require any decryption, or XOR with a card serial number. In step 2, a biocertificate is digitally signed and compared to a certificate by the issuer. In step 4, a predetermined data from a one-way function is compared to the holder details. Even if the Examiner is still of the belief that the digitally signed biocertificate is analogous to the recovered

checksum and that the predetermined data is analogous to the other checksum, then following the teachings of Chen, the digitally signed biocertificate would be compared with the predetermined data. However, as explained earlier, the predetermined data is compared to the holder details, not the biocertificate. The purpose of having the holder details separate from the biocertificate is so that the biometric data of the holder would not be directly linked to the holder details, which effectively deals with privacy concerns.

Furthermore, the Examiner cites a procedure as taught by Chen for authenticating the user (column 10, lines 13-31). This deals with step 3 and not steps 2 or 4. Chen teaches a procedure that requires entering a password assigned to the card. The password is then encrypted with the card's serial number to generate a PIN. This PIN is then compared to a PIN originally stored on the card. None of Applicant's steps require inputting a password by the user, which could be easily used by a person other than the intended user.

It is also well known to a person skilled in the art that a machine-readable zone refers to data printed on the external surface of a card. Machine-readable zones found on passports, visas, and other travel documents have been standardized by the ISO/IEC as having alphanumeric character sets in an optical recognition format. Claims 1, 5, 6, and 8 have also been amended to further clarify that the machine readable zone is provided "on the external surface of the card." Support for this amendment is found on page 5, lines 24-25 and Fig. 1 of Applicant's specification, as well as from the general knowledge of a person skilled in the art. None of the cited references teach or suggest a machine readable zone, or more specifically, a machine readable zone provided on the external surface of the card.

Applicant further submits that the rejections under 35 U.S.C. § 103 are inappropriate and that KSR applies to the instant application.

Applicant submits that there is no teaching, suggestion, motivation test promulgated by United States Court of Customs and Patent Appeals and adopted by the Federal Circuit. *Application of Bergel*, 292 F.2d 955, 956-957, 48 C.C.P.A. 1102, 1961 Dec. Comm'r Pat. 504 (1961). The Applicant recognized, however, that the current authority on matters of obviousness

must square with the Supreme Court's recent decision in *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 82 U.S.P.Q.2d 1385 (2007). Accordingly, although the teaching, suggestion, motivation test is still recognized under *KSR*, the test is largely subsumed by the more general principles laid out in *KSR*. Indeed, in any given application, the combination of elements "must do more than yield a predictable result." *Id.* at 1740. Nevertheless, combining elements "in an unexpected and fruitful manner" is sufficient to render an invention non-obvious. *Id.*

Any Teaching or Combination of References Used by the Examiner is Improper

*KSR* provides guidance with respect to the combination of references used to reject a patent application on the ground of obviousness. According to *KSR*: "Although **common sense** directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, **it can be important to identify a reason** that would have **prompted** a person of ordinary skill in the relevant field **to combine the elements** in the way the claimed new invention does." *KSR* at 1741 (emphasis added).

More importantly, "a patent composed of several elements **is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.**" *Id.* (emphasis added).

In *KSR*, the Supreme Court addressed such logic in obviousness-type rejections. Importantly, *KSR* specifically forbids obviousness rejections simply because each element was independently known in the prior art. The art cited against the instant application falls into this rubric because they are nothing more than a string of unrelated references showing each of the claimed elements with tenuous logic to support their combination.

The Examiner has failed in his burden to explain any compelling reason why a person of ordinary skill would have combined these references.

No Reasonable Expectation of Success Can Be Inferred from the Combination of References Asserted by the Examiner

Reasonable Expectation Standard Reaffirmed Post-KSR

The Federal Circuit stated “obviousness does not require absolute predictability of success . . . [a]ll that is required is a reasonable expectation of success.” *In re O’Farrell*, 853 F.2d 894, 903-04; 7 U.S.P.Q.2d 1673 (Fed. Cir. 1988). Thus, if a reasonable expectation of success is derived from a reference or combination of references, an invention may be rendered obvious. Conversely, where no reasonable expectation of success is derived, an obviousness rejection is improper. *Id.*

More specifically, *O’Farrell* provides general guidance as to when an invention falls under the reasonable expectation of success rubric, which was subsequently reaffirmed by the Federal Circuit post-KSR in *Pharmastem Therapeutics, Inc. v. Viacell, Inc.*, 491 F.3d 1342, 1364; 83 U.S.P.Q.2d 1289 (Fed. Cir. 2007). According to the Federal Circuit, “an invention would not be invalid for obviousness if the inventor would have been motivated ‘to **vary all parameters or try each of numerous possible choices until one possibly arrived at a successful result**, where the **prior art gave either no indication** of which parameters were critical or **no direction** as to which of many possible choices is likely to be successful.’” *Id.* at 1364, *quoting Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165, 77 U.S.P.Q.2d 1865 (Fed. Cir. 2006) (emphasis added).

In a secondary test posited by the Federal Circuit in *Pharmastem*, the court stated “[I]ikewise, an invention would **not be deemed obvious** if **all that was suggested** ‘was to **explore a new technology or general approach** that seemed to be a **promising field of experimentation**, where the **prior art gave only general guidance** as to the particular form of the claimed invention or how to achieve it.’” *Id.*, *quoting Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165, 77 U.S.P.Q.2d 1865 (Fed. Cir. 2006) (emphasis added).

No Reasonable Expectation of Success Where Numerous Possible Choices or Requirement to Vary All The Parameters

Using the first of the standards promulgated by the Federal Circuit, the combination of references cited by the Examiner against the claims have no reasonable expectation of success because the prior art references give no indication of critical parameters or direction as to how to achieve the claimed invention. Using any one of the prior art as the starting point to arrive at the claimed references cited against the instant application would require numerous choices in direction and experimentation, as well as variance of many parameters to arrive at the claimed invention.

For the reasons stated above, the prior art references cited against the claims also fail the second standard promulgated by the Federal Circuit. An invention is not obvious if all that was suggested is to explore a new technology or general approach that seemed to be a promising field of experimentation, where the prior art gave only general guidance as to the particular form of the claimed invention or how to achieve it. *Pharmastem* at 1364. In other words, the combination of references must give specific guidance to arrive at the claimed invention.

More specifically, the references cited against the instant claims include references directed to different fields of authentication and verification procedures. These references alone give no more than general guidance to the instant problem and claimed solution, and arguably do not give any guidance whatsoever.

In fact, the combination of these references makes sense **only** when viewed in the context of the specification and claims. Alone, they don't get a person of ordinary skill in the art any closer to an expectation of success because they simply don't have enough guidance, even when combined, to guide a person of ordinary skill in the art to the claimed result without significant detective work.

Combining Burger, Trench, and Chen in any manner does not result in the claimed limitations and elements of Applicant's invention. Applicant submits that the independent claims and the claims thereby dependent thereon are not obvious and are therefore patentable under 35 USC §103. The Examiner is respectfully requested to reconsider and now withdraw the Examiner's rejection.

**Conclusion**

In view of the above, it is respectfully submitted that this application is now in good order for allowance, and such early action is respectfully solicited. Should matters remain, which the Examiner believes could be resolved in a telephone interview, the Examiner is requested to telephone Applicant's undersigned attorney.

The Director is authorized to charge any additional fee(s) or any underpayment of fee(s), or to credit any overpayments to **Deposit Account Number 50-2638**. Please ensure that Attorney Docket Number 072998-012200 is referred to when charging any payments or credits for this case.

Respectfully submitted,



Daniel H. Wu  
Reg. No. 62,268

Date: November 3, 2008

GREENBERG TRAURIG, LLP  
2450 Colorado Avenue, Suite 400E  
Santa Monica, CA 90404  
Phone: (310) 586-7700  
Fax: (310) 586-7800  
E-mail: laipmail@gtlaw.com  
LA 127,660,468v1